5.1.2005

PONOVITEV:

(A,*) grupoid
$(a*b)*c = a*(b*c)$ asociativnost

Če je operacija asociativna, potem ima polgrupo

(A,*) polgrupa

e je enota/nevtralni element $a*e = e*a = a$

(A,*,e) monoid
ali (A,*)

$5*x=5*y$
$x=y$

(5 je poenostavljiv element)

obratni/inverzni elementi $a*a' = a'*a = e$

(A,*) grupa
ali (A,*,e)
ali …

NAPREJ:

Izrek:
Naj bo (A,*) monoid z enoto e.
Naj bosta $a,b \in A$ obrnljiva in a', b' njena obrata (inverza). Potem je tudi $a*b$ obrnljiv in $(a*b)' = b'*a'$

Dokaz: $(a*b) * (b'*a') = a*(b*b')*a' = a*e*a' = a*a' = e$
$(b'*a') * (a*b) = e$ (podobno)

Def.: Naj bo (A,*) grupoid
$a \in A$ je središčni (centralen), če za vse $b \in A$ velja:
$a*b=b*a$

Množico središčnih elementov imenujemo središče (center).

Trdimo: Naj bo (A,*) polgrupa. Središče polgrupe je trdna množica.

Dokaz: Če sta $a_1$ in $a_2$ središčna, potem je tudi $a_1*a_2$ središčni.
Če $a_1$ in $a_2$ komutirata z vsemi elementi structure, potem tudi $a_1*a_2$ komutira z vsemi elementi structure ← to dokazujemo.

$a_1$, $a_2$ središčna, $b \in A$ poljuben
Pokazati je treba: $b*(a_1*a_2) = (a_1*a_2)*b$ □

Računajmo: $b*(a_1*a_2) = b* a_1*a_2 = a_1*b*a_2 = a_1*a_2*b = (a_1*a_2)*b$

## 5. PODSTRUKTURE

(A,*) struktura (grupoid, polgrupa, monoid, grupa)

$B \subseteq A$, B neprazna in trdna množica. Kaj je (B,*)?

- če (A,*) grupoid, je (B,*) grupoid.
- če je (A,*) polgrupa je (B,*) polgrupa.
- če je (A,*) monoid z enoto e in če $e \in B$, potem je (B,*) monoid z isto enoto e.
- če je (A,*) grupa z enoto e in a' inverz elementa a, in če $e \in B$ in če z a-jem v B-ju najdemu tudi a', potem je (B,*) grupa z isto enoto in istimi inverzi.

Takemu (B,*) pravimo

POD grupoid
POD polgrupa
POD monoid
POD grupa v (A,*).

## 6. HOMOMORFIZMI IN IZOMORFIZMI

$S_1 = (\{ p, q, r, s \}, \circ)$

p...rotacija za 0°
q...rotacija za 90°
r...rotacija za 180°
s...rotacija za 270°

| ∘ | p | q | r | s |
|---|---|---|---|---|
| p | p | q | r | s |
| q | q | r | s | p |
| r | r | s | p | q |
| s | s | p | q | r |

$S_2 = (\{ 1, 2, 3, 4 \}, *)$

$x*y = x \cdot y \pmod 5$

| * | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

$h: \{ p, q, r, s \} \rightarrow \{ 1, 2, 3, 4 \}$
določen z

| x | p | q | r | s |
|---|---|---|---|---|
| h(x) | 1 | 2 | 4 | 3 |

| ∘ | p | q | s | r |
|---|---|---|---|---|
| p | p | q | s | r |
| q | q | r | p | s |
| s | s | p | r | q |
| r | r | s | q | p |

$S_1$ in $S_2$ sta izomorfni strukturi, h je izomorfizem struktur $S_1$ in $S_2$.

Def.: Preslikava $h:A\rightarrow B$ je homomorfizem grupoida $(A,\circ)$ v grupoid $(B,*)$, če za vse $x,y\in A$

$h(x\circ y) = h(x)*h(y)$

Zgled: 1) $(Z,+)$ $(\{0,1\},\underline{v})$
$h:Z\rightarrow\{0,1\}$
$n\mapsto(n \bmod 2)$
$2k\mapsto 0$
$2k+1\mapsto 1$

$h(n+m) = h(n)\ \underline{v}\ h(m)$

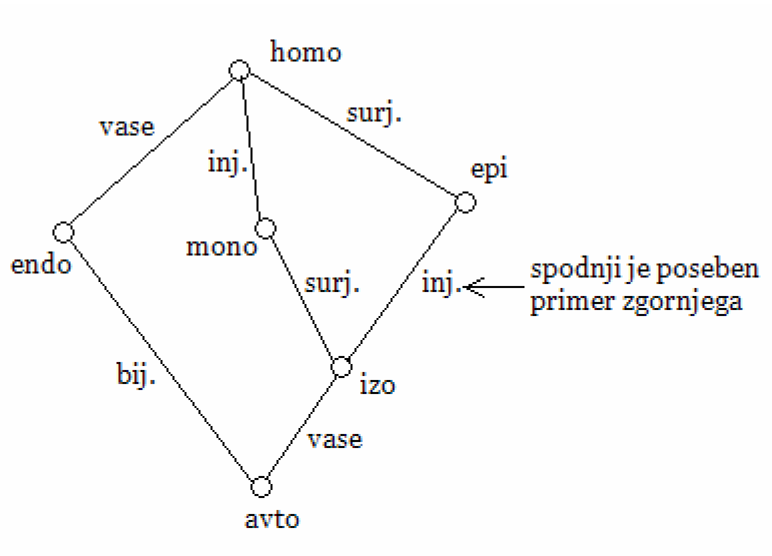
2) $(R,+)$ $((0,\infty),\cdot)$

2 izberemo

$h: R\rightarrow(0,\infty)$
$h(x) = 2^x$

$$\begin{array}{ccc} h(x+y) & = & h(x)\cdot h(y) \\ \| & & \| \\ 2^{x+y} & = & 2^x\cdot 2^y \end{array}$$

Def.: injektivni homomorfizem je monomorfizem,
surjektivni homomorfizem je epimorfizem,
bijektivni homomorfizem je izomorfizem,
homomorfizem vase je endomorfizem,
izomorfizem vase je avtomorfizem




<u>Izrek</u>: Če je homomorfizem $h: A \to B$ iz grupoida $(A,\circ)$ v grupoid $(B,*)$ surjektiven (epimorfizem), potem ohranja:

- splošne lastnosti operacije (če je $\circ$ asociativna, je tudi $*$ asociativna, podobno komutativnost)
- če je e enota v $(A,\circ)$, potem je h(e) enota v $(B,*)$.
- če je a' obrat a v $(A,\circ)$, potem je h(a') obrat h(a) v $(B,*)$

V tem primeru ima tudi $(B,*)$ vsaj tako lepo algebrsko strukturo kot $(A,\circ)$.

<u>Naloga</u>: Katera struktura je $((0,1),*)$, kjer je $*$ definirana z

$$a*b = \frac{a \cdot b}{1-a-b+2 \cdot a \cdot b}$$

$$a*(b*c) = (a*b)*c$$

Začnemo z $((0,\infty),\cdot)$

$h: (0,\infty) \to (0,1)$
$h: x \mapsto 1/(1+x)$ bijektivna preslikava (verjamemo)

Če izberemo poljubna $x, y \in (0,\infty)$,
$h(x \cdot y) = h(x)*h(y) = (1/(1+x)) * (1/(1+y)) =$

$$\| \qquad \frac{1}{1+x \cdot y}$$

$$\frac{\left(\frac{1}{1+x}\right)\left(\frac{1}{1+y}\right)}{1-\frac{1}{1+x}-\frac{1}{1+y}+2\frac{1}{1+x}\cdot\frac{1}{1+y}} = \frac{1}{(1+x)(1+y)-(1+y)-(1+x)+2} =$$

$$= \frac{1}{1+x+y+x\cdot y-1-y-1-x+2} = \frac{1}{1+x\cdot y}$$

Odgovor:
((0,1),*) je grupa, enota je h(1) = 1/(1+1) = ½
Kolikšen je a', če je a∈(0,1)?

h: x |-> a
h: 1/x |-> a'

a = 1/(1+x)
a' = 1/(1+1/x) = 1/(1+1/(1/a-1)) = 1/(1+1/((1-a)/a)) = 1/(1+a/(1-a)) = 1/((1-a+a)/(1-a)) = 1-a

1+x = 1/a, x = 1/a – 1

## 7. Kongruenčne relacije in homomorfizmi

Naj bo (A,*) grupoid in R ekvivalenčna relacija v A.
Vprašanje: Ali lahko * uporabimo tudi na A/R?

<u>Def.</u>: R je <u>kongruenčna relacija</u>, če je ∀x,y∈A.
[x],[y]∈A/R
[x] * [y] = [x*y] ← neodvisno od izbire predstavnikov ekvivalenčnih razredov.

Bolje: $xR\bar{x}$ in $yR\bar{y}$, potem je
(x*y)R(x * y)

<u>Zgled</u>: ({a,b,c,d,e},*)

| * | a | b | c | d | e |
|---|---|---|---|---|---|
| a | a | b | c | d | e |
| b | b | c | c | d | e |
| c | c | b | a | d | d |
| d | d | e | e | b | b |
| e | e | d | e | b | a |

A/R = { {a,b,c}, {d,e} }
α δ

| * | α | δ |
|---|---|---|
| α | α | δ |
| δ | δ | α |

<u>Zgled</u>: m∈N, m≥2.

Z, ekvivalenčna relacija na Z

$x \equiv y \pmod{m}$ …  m deli $x-y$
$(Z,+)$ je grupa
$(Z,\cdot)$ je monoid

$x \equiv y$ (mod m je kongruenčna relacija tako za + kot za $\cdot$.
$Z_m = Z/_{(\text{mod } m)} = \{[0],[1],[2], \ldots, [m-1]\}$

$x+y \equiv \bar{x} + \bar{y} \pmod{m}$, če:

$$\boxed{\begin{array}{ll} (*): & x \equiv \bar{x} \pmod{m} \\ & y \equiv \bar{y} \pmod{m} \end{array}}$$

po definiciji  m deli $x-\bar{y}$ } m deli $x - \bar{x} + y - \bar{y} =$

m deli $y-\bar{y}$ }  $= (x+y)-(\bar{x}+\bar{y})$

$x \cdot y \equiv \bar{x} \cdot \bar{y} \pmod{m}$, če (*)

$x \cdot y - x \cdot \bar{y} = x \cdot y - x \cdot \bar{y} + x \cdot \bar{y} - \bar{x} = x(y-\bar{y}) + \bar{y}(x-\bar{x})$

m deli člena zaradi (*)